REPUBLIQUE DU CAMEROUN
Paix – Travail – Patrie

AGENCE NATIONALE DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Centre de Réponse
Aux Incidents de Sécurité Informatique

REPUBLIC OF CAMEROON
Peace – Work – Fatherland

NATIONAL AGENCY FOR INFORMATION AND COMMUNICATION TECHNOLOGIES

Computer Incident Response Team

Bulletin de sécurité N°1 du mois de Mars 2025

B.P. 6170 Tél : 694 405 868 Web : http//www.antic.cm ; Email : infos@antic.cm

Sommaire

I. LEXIQUE DU BULLETIN

Expression	Signification
Date de publication	Date à laquelle la vulnérabilité a été officiellement publiée par le développeur ou constructeur de la ressource concernée.
Dernière version	Lien de téléchargement de la dernière version de la ressource concernée, dans le cas d'une ressource logicielle ou système d'exploitation.
Description	Présentation des détails sur la vulnérabilité, entre autre les versions de la ressource concernée par la vulnérabilité, le vecteur d'exploitation de la vulnérabilité (local, réseau …).
Référence CVE	CVE (Common Vulnerabilities and Exposures) est un annuaire de vulnérabilités de sécurité. Cet annuaire est maintenu par l'organisme MITRE, soutenu par le Département de la Sécurité intérieure des États-Unis. Les identifiants CVE sont des références de la forme CVE-AAAA-NNNN (AAAA est l'année de publication et NNNN un numéro incrémenté). Plus d'information à l'adresse : http://cve.mitre.org/
Score CVSS	CVSS (Common Vulnerability Scoring System) est un système d'évaluation des vulnérabilités qui permet d'associer une valeur (comprise entre 0 et 10) évaluant la criticité d'une vulnérabilité. CVSS fournit un cadre commun pour évaluer les niveaux de criticité, les caractéristiques et les impacts des vulnérabilités de sécurité informatique. Plus d'informations aux adresses : http://www.first.org/cvss/cvss-guide.html, http://www.cert-ist.com/fra/ressources/Publications_ArticlesBulletins/Veilletechnologique/CVSSv2/
Solution	Lien vers d'éventuelles solutions permettant de colmater ou de contourner la vulnérabilité.
Vulnérabilité	Faille de sécurité publiée, Synopsis de la faille, généralement sur la forme « Vulnérabilité dans X » où X est une ressource informatique, matérielle, logicielle ou système d'exploitation concernée par la vulnérabilité.

II. VULNÉRABILITÉS PUBLIÉES

II.1 NAVIGATEURS

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Microsoft Edge	De multiples vulnérabilités ont été découvertes dans Microsoft Edge. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Microsoft indique que la vulnérabilité CVE-2025-24201 est activement exploitée. Les versions affectées sont les suivantes : • Microsoft Edge versions antérieures à 134.0.3124.62	13/03/2025	CVE-2025-24201	134.0.3124.62 Télécharger	Mettre à jour le navigateur	8.8
Vulnérabilité dans Google Chrome	De multiples vulnérabilités ont été découvertes dans Google Chrome. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Les versions affectées sont les suivantes : • Chrome Extended Stable versions antérieures à 134.0.6998.89 pour Windows et	11/03/2025	CVE-2025-2137	134.0.6998.88/.89 Télécharger	Mettre à jour le navigateur	NA

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
	Mac • Chrome versions antérieures à 134.0.6998.88 pour Linux • Chrome versions antérieures à 134.0.6998.88/.89 pour Windows et Mac					

II.2 SYSTÈMES D'EXPLOITATION

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans le noyau Linux de Red Hat	De multiples vulnérabilités ont été découvertes dans le noyau Linux de Red Hat. Elles permettent à un attaquant de provoquer une exécution de code arbitraire, une atteinte à la confidentialité des données et un déni de service.	14/03/2025	CVE-2024-57807	9.4 Essayer	Veuillez-vous référer au Bulletin de sécurité : https://access.redhat.com/errata/RHSA-2025:2646	5.5

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans le noyau Linux de SUSE	De multiples vulnérabilités ont été découvertes dans le noyau Linux de SUSE. Certaines d'entre elles permettent à un attaquant de provoquer une élévation de privilèges, une atteinte à la confidentialité des données et une atteinte à l'intégrité des données.	14/03/2025	CVE-2025-21802	15 SP6 Essayer	Veuillez-vous référer au Bulletin de sécurité : https://www.suse.com/support/update/announcement/2025/suse-su-20250856-1	NA
Vulnérabilité dans le noyau Linux d'Ubuntu	De multiples vulnérabilités ont été découvertes dans le noyau Linux d'Ubuntu. Certaines d'entre elles permettent à un attaquant de provoquer une atteinte à la confidentialité des données, une atteinte à l'intégrité des données et un contournement de la politique de sécurité. Les systèmes affectés sont les suivants : • Ubuntu 14.04 ESM • Ubuntu 16.04 ESM • Ubuntu 18.04 ESM • Ubuntu 22.04 LTS • Ubuntu 24.04 LTS	14/03/2025	CVE-2024-56672	Ubuntu 24.10 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://ubuntu.com/security/notices/USN-7344-2	7.8

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans le noyau Linux de Debian	De multiples vulnérabilités ont été découvertes dans le noyau Linux de Debian LTS. Elles permettent à un attaquant de provoquer une élévation de privilèges, une atteinte à la confidentialité des données et un déni de service. Les systèmes affectés sont les suivants : • Debian LTS bullseye versions antérieures à 5.10.234-1 • Debian LTS bullseye versions antérieures à 6.1.128-1~deb11u1	07/03/2025	CVE-2025-21699	12.10.0 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://lists.debian.org/debian-lts-announce/2025/03/msg00001.html	5.5
Vulnérabilité dans Juniper Networks Junos OS	Une vulnérabilité a été découverte dans Juniper Networks Junos OS. Elle permet à un attaquant de provoquer une exécution de code arbitraire. Les systèmes affectés sont les suivants : • Junos OS versions 23.4.x antérieures à 23.4R2-S4 • Junos OS versions 24.2.x antérieures à 24.2R1-S2 ou 24.2R2 • Junos OS versions antérieures à 21.2R3-S9	13/03/2025	CVE-2025-21590	21.2R3-S9 Explorer	Veuillez-vous référer au Bulletin de sécurité : https://supportportal.juniper.net/s/article/2025-03-Out-of-Cycle-Security-Bulletin-Junos-OS-A-local-attacker-with-shell-access-can-execute-arbitrary-code-CVE-2025-21590	6.7

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilités dans Microsoft Windows	De multiples vulnérabilités ont été découvertes dans Microsoft Windows. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, une élévation de privilèges et une atteinte à la confidentialité des données. Microsoft indique que les vulnérabilités CVE-2025-24983, CVE-2025-24984, CVE-2025-24985, CVE-2025-24991, CVE-2025-24993 et CVE-2025-26633 sont activement exploitées.	12/03/2025	CVE-2025-26633	Microsoft Windows 11	Veuillez-vous référer au Bulletin de sécurité : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21420	7.0
Vulnérabilité dans Google Android	De multiples vulnérabilités ont été découvertes dans Google Android. Elles permettent à un attaquant de provoquer une élévation de privilèges, une atteinte à la confidentialité des données et un déni de service Les systèmes affectés sont les suivants : • Google Pixel sans les correctifs de sécurité du 5 mars 2025	05/03/2025	CVE-2025-22377	16 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://source.android.com/docs/security/bulletin/pixel/2025-03-01?hl=fr	NA

II.3 CMS

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Joomla	Une vulnérabilité a été découverte dans Joomla!. Elle permet à un attaquant de provoquer une exécution de code arbitraire à distance. Les versions affectées sont les suivantes : • Joomla! CMS versions 4.x antérieures à 4.4.12 • Joomla! CMS versions 5.x antérieures à 5.2.5	12/03/2025	CVE-2025-22213	5.2.5 Télécharger	Mettre à jour le navigateur	5.4

II.4 AUTRES

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans PHP	De multiples vulnérabilités ont été découvertes dans PHP. Certaines d'entre elles permettent à un attaquant de provoquer un déni de service à distance, une atteinte à la confidentialité des données et un contournement de la politique de sécurité. Les versions affectées sont les suivantes : • PHP versions 8.3.x antérieures à 8.3.19 • PHP versions 8.4.x antérieures à 8.4.5	14/03/2024	CVE-2025-1861	8.4.5 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://www.php.net/ChangeLog-8.php#8.4.5	4.3
Vulnérabilité dans Microsoft Dataverse	Une vulnérabilité a été découverte dans Microsoft Dataverse. Elle permet à un attaquant de provoquer une élévation de privilèges. Les systèmes affectés sont les suivants : • Microsoft Dataverse	14/03/2025	CVE-2025-24053	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24053	7.2

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilités dans GitLab	De multiples vulnérabilités ont été découvertes dans GitLab. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, un déni de service à distance et une atteinte à la confidentialité des données. Les versions affectées sont les suivantes : • GitLab Community Edition (CE) et Enterprise Edition (EE) versions 17.9.x antérieures à 17.9.2	13/03/2025	CVE-2025-27407	17.9.2 Explorer	Veuillez-vous référer au Bulletin de sécurité : https://about.gitlab.com/releases/2025/03/12/patch-release-gitlab-17-9-2-released/	9.0
Vulnérabilités dans Apache Tomcat	Une vulnérabilité a été découverte dans Apache Tomcat. Elle permet à un attaquant de provoquer une exécution de code arbitraire à distance, une atteinte à la confidentialité des données et une atteinte à l'intégrité des données. Les versions affectées sont les suivantes : • Tomcat versions 10.1.x antérieures à 10.1.35 • Tomcat versions 11.0.x antérieures à 11.0.3	12/03/2025	CVE-2025-24813	11.0.5 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.99	NA

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilités dans les produits Fortinet	De multiples vulnérabilités ont été découvertes dans les produits Fortinet. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, une élévation de privilèges et une atteinte à la confidentialité des données.	12/03/2025	CVE-2024-55597	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://www.fortiguard.com/psirt/FG-IR-24-439	5.5
Multiples vulnérabilités dans Nagios XI	Une vulnérabilité a été découverte dans Nagios XI. Elle permet à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Les systèmes affectés sont les suivants : • Nagios XI versions antérieures à 2024R1.4	07/03/2025		2024R1.4 Explorer	Veuillez-vous référer au Bulletin de sécurité : https://www.nagios.com/changelog/	

II.4 ACTUALITES

1. **Women Empowerment in Cybersecurity 2025 : les femmes au cœur de la cybersécurité en Côte d'Ivoire**
   Orange Digital Center accueille un événement d'envergure le ***mardi 11 mars 2025*** en Côte d'Ivoire au Plateau. Il s'agit du ***Women Empowerment in Cybersecurity (WEC).*** Organisé par ***Diamond Security Consulting***, ce forum ambitionne de promouvoir la participation des femmes dans un secteur encore largement dominé par les hommes. Face aux inégalités de genre dans le domaine de la **cybersécurité,** le WEC entend sensibiliser les femmes aux opportunités qu'offre ce secteur en pleine croissance et faciliter leur insertion professionnelle. L'événement réunira des experts, des recruteurs et des représentants d'institutions gouvernementales afin de favoriser une meilleure inclusion des talents féminins et de créer des opportunités concrètes pour celles qui souhaitent s'engager dans ce domaine.
   https://cybersecuritymag.africa/index.php/women-empowerment-cybersecurity-2025-en-cote-divoire

2. **La NITA-U renforce l'armée contre les cybermenaces en Ouganda**
   La National Information Technology Authority de l'Ouganda (NITA-U) a clôturé ce jeudi 06 mars 2025 une formation intensive d'une semaine sur la cybersécurité à l'intention de 50 membres des forces de défense ougandaises (UPDF). Un pari stratégique, selon les experts, pour sécuriser les infrastructures sensibles face à des menaces de plus en plus sophistiquées. Selon les experts de la NITA-U, cette formation est dans son troisième cycle. Elle a été conçue sur le modèle « train the trainer » et vise à créer un réseau de référents capables de diffuser les bonnes pratiques en matière de sécurité des données et de réponse aux incidents. Les modules de la formation ont été dirigés sur la gestion des vulnérabilités, l'analyse de risques et les protocoles de cybersurveillance.
   https://cybersecuritymag.africa/index.php/la-nita-u-renforce-larmee-contre-les-cybermenaces-en-ouganda

3. **Le Rwanda envisage le lancement d'une académie de cybersécurité pour renforcer la sécurité numérique**

   Le gouvernement rwandais s'apprête à franchir une nouvelle étape dans la lutte contre les cybermenaces. Le pays envisage mettre en place une académie dédiée à la cybersécurité avant la fin de cette année. L'annonce a été faite par Paula Ingabire, Ministre des TIC et de l'Innovation, le jeudi 13 mars 2025 au cours d'une session parlementaire sur l'information, la communication et la technologie.

   https://cybersecuritymag.africa/index.php/rwanda-envisage-le-lancement-academie-de-cybersecurite

4. **De l'inégalité à l'inclusion : le WEC 2025 ouvre la voie aux femmes dans la cybersécurité**
   Le 11 mars 2025, Orange Digital Center à Abidjan a servi de cadre à une initiative d'envergure en faveur de l'autonomisation des femmes dans la cybersécurité. Le forum Women Empowerment in Cybersecurity (WEC), organisé par Diamond Security Consulting, a rassemblé des leaders du secteur, des recruteurs et des représentants gouvernementaux. L'objectif principal : accroître la participation des femmes dans un domaine où elles restent sous-représentées. Laïcana Coulibaly, CEO de Diamond Security Consulting et commissaire général de l'événement, a souligné : « L'inclusion des femmes en cybersécurité n'est pas un luxe mais une nécessité ».
   https://cybersecuritymag.africa/index.php/wec-2025-ouvre-la-voie-aux-femmes-dans-la-cybersecurite

5. **Cyberharcèlement et violences en ligne : l'ONG Woezon Digital Inclusion Bridge (WDIB) organise un webinaire**
   L'ONG Woezon Digital Inclusion Bridge (WDIB) organise un webinaire le mercredi 19 mars 2025. Ce webinaire est intitulé "Cyber-harcèlement, Violences Basées sur le Genre : Stratégies Essentielles pour Protéger Votre Vie Numérique". Il sera consacré aux techniques essentielles pour contrer le cyberharcèlement et les violences basées sur le genre. Cette initiative s'inscrit dans la dynamique de sécurisation de la vie numérique en Afrique. Cet événement virtuel est un rendez-vous incontournable pour quiconque souhaite naviguer sereinement dans un environnement numérique de plus en plus complexe. Pour les organisateurs, ce webinaire se présente comme une bouffée d'oxygène pour les utilisateurs d'Internet particulièrement les femmes et les personnes handicapées.
   https://cybersecuritymag.africa/index.php/cyberharcelement-et-violences-en-ligne-long-woezon-digital-inclusion-bridge-organise-webinaire

6. **La sécurisation des identités machines, une priorité pour 77% des responsables de sécurité français**
   CyberArk, le leader mondial de la sécurité des identités, publie son rapport sur l'état de la sécurité des identités machines dévoilant que les incidents de sécurité liés aux identités machines sont en augmentation, alors que le volume et la complexité de ces identités ne cessent de se multiplier. 64 % des organisations françaises ont connu au moins une panne liée aux certificats au cours de l'année écoulée, ce qui représente une augmentation significative par rapport aux années précédentes. De plus, 37 % des responsables de sécurité français ont signalé des incidents ou des violations de sécurité dus à des identités machines compromises.
   https://www.undernews.fr/reseau-securite/la-securisation-des-identites-machines-une-priorite-pour-77-des-responsables-de-securite-francais.html

III. NOTES IMPORTANTES

1. Veuillez enregistrer les adresses, alerts@cirt.cm et alerts@cirt.antic.cm parmi vos contacts ou l'enregistrer comme expéditeur approuvé afin de ne plus recevoir les mails en provenance de cette adresse dans vos spam.
2. Ce document est produit régulièrement et téléchargeable sur notre site web www.cirt.cm . Vous y trouverez aussi des alertes et autres publications relatives à la cybersécurité et à la cybercriminalité.
3. CentOS 8 n'est plus supporté depuis la fin de l'année 2021. Si votre organisation n'a pas encore effectué une migration vers une version supportée notamment CentOS 8 ou 9 Stream (voir https://www.centos.org/centos-stream/) alors, votre système d'information court de grands risques. En outre, le cycle de vie des versions de CentOS 7 a été prolongé jusqu'en Juin 2024. L'utilisation des solutions ne possédant aucun support technique présente un risque élevé étant donné qu'aucun correctif ne sera émis après d'éventuelles vulnérabilités détectées sur celles-ci.
4. Microsoft a mis fin au support de toutes les versions de Windows 7 depuis le 14 janvier 2020. Depuis cette date les systèmes fonctionnant sous Microsoft Windows 7 ne reçoivent plus le support technique, les mises à jour et les correctifs de sécurité. Il est recommandé aux différents Organismes de planifier la migration des postes utilisateurs utilisant encore ce système vers une version supportée de Microsoft Windows, notamment en prenant en compte cette migration dans les prévisions budgétaires.

   https://support.microsoft.com/fr-ma/help/4057281/windows-7-support-will-end-on-january14-2020
5. Afin de se prémunir au maximum d'éventuelle attaques informatiques pouvant endommager tout ou partie de vos systèmes, vous devez mettre à jour tous vos systèmes et logiciels utilisés. Nous vous recommandons donc de télécharger et d'installer toutes les dernières versions de logiciels et systèmes utilisés, uniquement sur les sites des constructeurs. Car tout logiciel téléchargé d'une source autre que celle du constructeur est potentiellement compromise par des malware et chevaux de Troie.

   Par ailleurs, si vous rencontrez quelques difficultés que ce soit dans l'application des correctifs susmentionnés ou ailleurs vous pouvez nous contacter à travers l'adresses email alerts@cirt.antic.cm ou au numéro de téléphone **8202**.